

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN RE SOLARWINDS CORPORATION
SECURITIES LITIGATION

§
§
§
§
§
§
§

MASTER FILE NO. 1:21-CV-138-RP

**DEFENDANTS SOLARWINDS AND BROWN'S
REPLY BRIEF IN SUPPORT OF MOTION TO DISMISS**

Paul R. Bessette
Texas Bar No. 02263050
Michael J. Biles
Texas Bar No. 24008578
KING & SPALDING LLP
500 W. 2nd Street, Suite 1800
Austin, TX 78701
Tel: (512) 457-2050
Fax: (512) 457-2100
pbessette@kslaw.com
mbiles@kslaw.com

*Counsel for SolarWinds Corp.
and Tim Brown*

TABLE OF CONTENTS

INTRODUCTION.....	1
I. PLAINTIFF FAILS TO PLEAD A STRONG INFERENCE OF SCIENTER.	2
A. Allegations that Brown was responsible for cybersecurity do not support a strong inference of scienter.	2
B. Allegations about the third-party Update Server password fail to raise a strong inference of scienter.	5
C. Thornton-Trump’s presentation does not support an inference of scienter.	7
D. Hindsight allegations that SolarWinds delayed spending on cybersecurity fail to plead scienter.	11
II. PLAINTIFF PLEADS NO MATERIAL FALSE OR MISLEADING STATEMENT.....	12
A. Plaintiff fails to plead that the Security Statement was false or misleading.	12
B. Plaintiff has not pled that optimistic opinion statements about SolarWinds’ cybersecurity were material.	13
III. PLAINTIFF FAILS TO PLEAD A CAUSAL LINK BETWEEN THE “CORRECTIVE DISCLOSURES” AND THE CYBERATTACK.	14
CONCLUSION.....	15

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>ABC Arbitrage Plaintiffs Grp. v. Tchuruk</i> , 291 F.3d 336 (5th Cir. 2002).....	4
<i>Abrams v. Baker Hughes Inc.</i> , 292 F.3d 424 (5th Cir. 2002).....	2, 9
<i>In re AFC Enters., Inc. Sec. Litig.</i> , 348 F. Supp. 2d 1363 (N.D. Ga. 2004)	11
<i>In re Akorn, Inc. Sec. Litig.</i> , 240 F. Supp. 3d 802 (N.D. Ill. 2017)	11
<i>In re ArthroCare Corp. Sec. Litig.</i> , 726 F. Supp. 2d 696 (W.D. Tex. 2010)	5, 6
<i>In re BP p.l.c. Sec. Litig.</i> , 843 F. Supp. 2d 712 (S.D. Tex. 2012)	4
<i>In re Dell Inc., Sec. Litig.</i> , 591 F. Supp. 2d 877 (W.D. Tex. 2008)	15
<i>In re Equifax Inc. Sec. Litig.</i> , 357 F. Supp. 3d 1189 (N.D. Ga. 2019)	10, 11, 14, 15
<i>In re First Am. Fin. Corp. Sec. Litig.</i> , No. 20-9781, 2021 WL 4807648 (C.D. Cal. Sept. 22, 2021)	13
<i>In re Heartland Payment Sys., Inc. Sec. Litig.</i> , No. 09-1043, 2009 WL 4798148 (D.N.J. Dec. 7, 2009)	2, 3, 6, 7
<i>Jaroslavic v. MeT Bank Corp.</i> , 962 F.3d 701 (3d Cir. 2020)	14
<i>Lormand v. US Unwired, Inc.</i> , 565 F.3d 228 (5th Cir. 2009).....	14
<i>In re Marriott Int’l, Inc. Customer Data Sec. Breach Litig. Sec. Actions</i> , No. 8:19-md-2879, 2021 WL 2407518 (D. Md. June 11, 2021)	3, 9, 10
<i>Nathenson v. Zonagen Inc.</i> , 267 F.3d 400 (5th Cir. 2001).....	2

<i>In re New Century</i> , 588 F. Supp. 2d 1206 (C.D. Cal. 2008)	7, 8, 12
<i>Plotkin v. IP Axxess Inc.</i> , 407 F.3d 690 (5th Cir. 2005).....	5, 6
<i>Pub. Emps. Ret. Sys. of Miss. v. Amedisys, Inc.</i> , 769 F.3d 313 (5th Cir. 2014).....	15
<i>In re Resideo Techs., Inc., Sec. Litig.</i> , 2021 WL 1195740 (D. Minn. Mar. 30, 2021)	12
<i>Santa Fe Indus. v. Green</i> , 430 U.S. 462 (1977).....	5
<i>Tuchman v. DSC Commc’ns Corp.</i> , 14 F.3d 1061 (5th Cir. 1994).....	9
<i>Yang v. Nobilis Health Corp.</i> , No. 20-20538, 2021 WL 3619863 (5th Cir. Aug. 13, 2021)	2, 3
<i>Zucco Partners, LLC v. Digimarc Corp.</i> , 552 F.3d 981 (9th Cir. 2009).....	3

INTRODUCTION

Plaintiff's Opposition to Defendants' Motions to Dismiss (the "Opposition" or "Opp.") repeats allegations by former employees who criticize SolarWinds' security practices and relies heavily on Ian Thornton-Trump's "Creating Security" presentation to several non-party executives 18 months before the Class Period started. These allegations fail to plead the particularized facts necessary to raise a strong inference that any defendant knew any of the challenged statements were false or spoke with severe recklessness. Thornton-Trump left SolarWinds 17 months before the Class Period began, and the other former employees served in sales, customer support, or HR functions—not internal security or software development functions. None of these witnesses can credibly speak to the cybersecurity measures in place at SolarWinds during the Class Period, and they add nothing to the element of scienter because Plaintiff does not allege that any former employee, including Thornton-Trump, communicated anything to any Individual Defendant. Further, the actual contents of Thornton-Trump's "Creating Security" presentation belie Plaintiff's mischaracterization that the presentation somehow shows that the SolarWinds Defendants spoke with severe recklessness. The presentation does not identify any alleged deficiency that conflicts with the statements Plaintiff alleges were false or misleading, or that made SolarWinds more vulnerable to a cyberattack than any other company.

Plaintiff's allegations also fail to plead facts linking the alleged security deficiencies with the cyberattack at issue—the Foreign Intelligence Service of the Russian Federation's ("SVR"), injection of malware into certain new releases of SolarWinds' Orion product in what has been dubbed "the largest and most sophisticated" cyber espionage operation in history (the "Cyberattack"). The most the Opposition offers is conclusory speculation that "a malicious actor ***could have*** uploaded malware" by using a "solarwinds123" password to access a third-party server (the "Update Sever"). Opp. at 2 (emphasis added). But multiple documents cited in the Complaint confirm that the Update

Server (i) was not part of SolarWinds’ internal IT architecture; (ii) could not be used to access SolarWinds’ internal systems; and (iii) was not used to distribute the compromised Orion products. These are not “alternative facts” offered by Defendants—they are set forth in the very documents that Plaintiff relies on in the Complaint. Moreover, Plaintiff’s speculative and conclusory allegations that the Update Server “could have” been the source of the Cyberattack are not pled with the factual specificity required under the PSLRA, Rule 9(b), or even Rule 8.

Plaintiff has failed to plead scienter, falsity, and loss causation, and the Court should therefore dismiss the Complaint.

I. PLAINTIFF FAILS TO PLEAD A STRONG INFERENCE OF SCIENTER.

A. Allegations that Brown was responsible for cybersecurity do not support a strong inference of scienter.

Plaintiff argues that, because Brown led security at SolarWinds, spoke publicly about cybersecurity, and believed it was important to SolarWinds, it follows that he must have known that statements challenged in the Complaint misrepresented “the true state of cybersecurity at SolarWinds.” Opp. at 46–48; 51–52. But the law is clear that conclusory allegations that a defendant must have known alleged facts based on his role or the importance of the facts to the company’s business fail to plead scienter.¹ Rather, to meet the PSLRA’s exacting scienter pleading standard, a plaintiff must plead particular facts establishing the defendant’s contemporaneous knowledge (or severely reckless disregard) of facts making the challenged statements materially false or misleading.²

¹ See *Yang v. Nobilis Health Corp.*, No. 20-20538, 2021 WL 3619863, at **2–3 (5th Cir. Aug. 13, 2021) (defendant’s position and “day-to-day” involvement did not support a strong inference of scienter); *Nathenson v. Zonagen Inc.*, 267 F.3d 400, 424 (5th Cir. 2001) (similar); see also *In re Heartland Payment Sys., Inc. Sec. Litig.*, No. 09–1043, 2009 WL 4798148, at *7 (D.N.J. Dec. 7, 2009) (holding that officers are not presumed to be familiar with facts just because they are “important to the company’s business.”).

² See *Heartland*, 2009 WL 4798148, at *7 (“[I]here must be other, individualized allegations that further suggest that the officer had knowledge of the [contrary] fact in question.”); accord *Abrams v. Baker Hughes Inc.*, 292 F.3d 424, 432–33 (5th Cir. 2002).

The Opposition identifies no such allegations. Instead, Plaintiff merely repeats conclusory and unsupported assertions, already debunked in the SolarWinds Defendants’ opening brief, that the Court should infer scienter because SolarWinds purportedly (i) lacked a security team; (ii) had no password policy; (iii) failed to “segment” its networks; (iv) did not conduct cybersecurity training; and (v) did not conduct background checks on new hires. *See* Opp. at 47 (citing Compl. ¶¶ 113-49).

Many of these claims are based on allegations attributed to Thornton-Trump. *See* Compl. ¶ 114 (“no security team”); ¶¶ 121 & 123 (allegations about passwords); ¶ 125 (no cybersecurity training); ¶ 132 (lack of network segmentation). But Plaintiff alleges that Thornton-Trump resigned from SolarWinds in May 2017—roughly 17 months before the start of the Class Period. *Id.* ¶ 88. He has no knowledge of SolarWinds’ security posture *during the Class Period*, nor of what Brown (who was hired *after* Thornton-Trump’s resignation) knew of such matters, and his allegations thus fail to support an inference of Brown’s (or any Defendant’s) scienter.³

The “former employee” (“FE”) allegations (Compl. ¶ 115, ¶¶ 118–22, ¶¶ 126–30, ¶¶ 133–49) fail to rescue Plaintiff’s claims. These allegations say nothing at all about what Defendants Brown and Thompson (the only alleged speakers) knew or recklessly disregarded concerning the alleged security matters and fail, for that reason alone, to support an inference of scienter.⁴ Plaintiff does not allege that any FE, including Thornton-Trump, shared concerns with Brown or Thompson. And Plaintiff’s argument that the FE allegations “corroborate” Thornton-Trump’s pre-Class Period critiques of SolarWinds’ cybersecurity practices is wrong. The FEs (former customer-facing sales/support or human resources staff) had no alleged responsibility for or expertise concerning SolarWinds’ internal

³ *See Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 996 (9th Cir. 2009) (witnesses who “were not employed . . . during the time period in question” did not support a strong inference of scienter).

⁴ *See Nobilis*, 2021 WL 3619863, at *2 (confidential witness allegations were silent as to “how or when [defendants] became aware of the relevant information” and thus failed to support an inference of scienter); *accord In re Marriott Int’l, Inc. Customer Data Sec. Breach Litig. Sec. Actions*, No. 8:19-md-2879, 2021 WL 2407518, at *35 (D. Md. June 11, 2021); *Heartland*, 2009 WL 4798148, at *8.

cybersecurity and therefore lack a reliable basis on which to speak to matters such as the existence of a security team or SolarWinds' password and network segmentation policies and practices.⁵ Nor does the alleged inability of some of these FEs to recall security training establish that there was no training during the Class Period. *See* Def. Br. at 22 & n.21. Further, the allegation that SolarWinds did not conduct background checks on new hires fails to raise a strong inference that Brown intended to deceive investors or acted severely recklessly in approving a statement that "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent detect and respond to security incidents."⁶

Finally, Plaintiff's effort to analogize this case to *In re BP p.l.c. Sec. Litig.*, 843 F. Supp. 2d 712 (S.D. Tex. 2012), *Opp.* at 47, fails. *BP* arose from the 2010 Deepwater Horizon oil rig disaster. The plaintiffs alleged that BP's CEO claimed to be intensely focused on implementing safety improvements in the wake of an earlier high-profile refinery explosion. The court therefore found it reasonable to infer that the CEO would (or should) have known that the company: (i) failed to implement numerous safety procedures recommended by regulators; (ii) received over one hundred citations from safety regulators in a four-year span; and (iii) prepared an internal analysis warning of "major process safety concerns in the Gulf of Mexico"—where the catastrophic Deepwater Horizon oil spill eventually occurred. *BP*, 843 F. Supp. 2d at 728, 733–34. Here, Plaintiff does not point to scores of regulatory citations, widespread failures to adopt recommended safety measures, or internal analyses warning of "major process safety concerns," but instead relies on allegations that: (i) a small number of former sales/HR employees were unaware of SolarWinds' security team and could not

⁵ *See ABC Arbitrage Plaintiffs Grp. v. Tchuruk*, 291 F.3d 336, 353 (5th Cir. 2002) (To be given any weight, confidential sources must be described "with sufficient particularity to support the probability that a person in the position occupied by the source ... would possess the information pleaded.").

⁶ The NIST Framework does not mandate compliance with every suggested guideline. Rather, it provides "guidance" that "should be customized by different sectors and individual organizations to best suit their risks, situations, and needs." Biles Decl. Ex. 23, NIST webpage at 1.

recall cybersecurity training; (ii) one former “sales engineer” was able to access unspecified “parts” of SolarWinds’ software development environment; (iii) the Company’s password policy may have been violated in certain instances; and (iv) SolarWinds did not conduct background checks on new hires (which it had no obligation to do). *See generally* Compl. ¶¶ 115–49. *BP* is not remotely apposite and fails to support a finding that Plaintiff has pled scienter here.

B. Allegations about the third-party Update Server password fail to raise a strong inference of scienter.

Plaintiff argues it has pled a strong inference of Brown’s scienter by alleging that he learned, on November 19, 2019, that the password (“solarwinds123”) to a third-party Update Server used to download certain SolarWinds software updates had been posted to a publicly accessible web page. Opp. at 48-51. This argument fails for several reasons.

Contrary to the Opposition’s conclusory and unsupported assertions (Opp. at 48), nothing alleged about the November 2019 notice regarding the Update Server password suggests that SolarWinds lacked a password policy. Nor do the allegations conflict with any challenged statement. At most, Plaintiff’s allegations plead a mistake or misjudgment by the intern who posted the password on a public site. *See* Def. Br. at 25.⁷ Accordingly, this case is not at all like *In re ArthroCare Corp. Sec. Litig.*, 726 F. Supp. 2d 696 (W.D. Tex. 2010) (alleging CEO ignored numerous public “red flags” signaling widespread health insurance billing fraud and accounting abuses in advance of financial restatements that reduced one year’s net income by 99%) or *Plotkin v. IP Access Inc.*, 407 F.3d 690 (5th Cir. 2005) (alleging misleading statements trumpeting multimillion dollar product purchase agreements from a customer that obviously lacked the financial wherewithal to make good on the purchase

⁷ The SolarWinds Defendants’ opening brief did not say that an intern *set the Update Server password*, but rather that an intern *posted* the password on the GitHub website. *Compare* Opp. at 49 *with* Def. Br. at 23, 25. Regardless, the allegation that SolarWinds “tasked an intern to set the password” at most pleads a managerial judgment that could, in hindsight, be questioned—not fraudulent conduct actionable under Section 10(b). *See Santa Fe Indus. v. Green*, 430 U.S. 462, 479-80 (1977).

commitments and filed for bankruptcy shortly thereafter). Unlike those cases, nothing alleged about the November 2019 Update Server password notice suggests “egregious refusal [by Brown] to see the obvious or investigate the doubtful.” Opp. at 48–49. To the contrary, Plaintiff alleges that Brown and SolarWinds “changed the password” and “fixed the issue within the same hour it was reported.” Compl. ¶ 112. That is the opposite of the “willful[] blindness” alleged in *ArthroCare* and *Plotkin*, and demonstrates that SolarWinds, in fact, had and enforced a password policy.

Plaintiff also erroneously argues that an inference of scienter arises because Brown “continued to direct investors and the public to his Security Statement” after being notified of the exposed Update Server password and promptly “fix[ing] the issue” in November 2019. The court in *Heartland* addressed similar (but much stronger) allegations and found them insufficient to plead either scienter or even a misleading statement. See Def. Br. at 24; see also *Heartland*, 2009 WL 4798148, at **4–8. In *Heartland*, the plaintiff alleged defendants knew about, but failed to disclose, that the company sustained a Structured Query Language (“SQL”) attack in which hackers inserted malware into the company’s network, eventually enabling the theft of 130 million credit and debit card numbers. *Id.* at **1–2, *8. The court held that none of the challenged statements—made *after* the company learned about the SQL attack, but *before* it learned of the data theft—were misleading for omitting the SQL attack, and that defendants had no duty under Section 10(b) to publicly report the SQL attack. *Id.* at **3–7. Addressing scienter, the court noted that the complaint alleged only that “a handful of lower-level employees” “believed that the company had not adequately addressed the SQL attack” and failed to plead that concerns were relayed to the defendants. *Id.* at **7–8. The court found those allegations inadequate: “Assuming that Defendants were aware of the SQL attack, it does not follow necessarily that they believed that Heartland’s security systems were deficient or that any problems created by the SQL attack had not been addressed.” *Id.* at *8.

Here, the Complaint does not allege that the Update Server password was used to compromise SolarWinds' network and gain access to the Orion build process through which the Cyberattack was carried out. *See* Def. Br. at 23–24. Indeed, in a March 2021 interview from which Plaintiff selectively quotes (Compl. ¶ 112), Brown explained that the Update Server was an FTP site separate from SolarWinds' system, and had nothing to do with the Sunburst Cyberattack:

The well-reported “SolarWinds123” password was unrelated to the attack. “It was a system with a separate username and password and nothing to do with Active Directory - that’s why it didn’t meet our password policies,” Brown said. “It was a separate FTP site and nothing to do with Sunburst. . . . [S]omebody posted a username and password in their own GitHub account that was public, a researcher reported it, we saw, fixed it, brought it under control and made sure it won’t happen again.”

“It was completely separate from the build system or the service account. It happened, and we fixed it within the same hour it was reported. It was a system outside of policy and had nothing to do with corporate identity systems,” he explained.

See Biles Decl. Ex. 32, iTWire (March 29, 2021) (emphasis added).⁸ But as the *Heartland* ruling makes clear, even if Plaintiff had pled facts alleging that the Update Server password was exploited in the Cyberattack, there still would be no inference of scienter, because there are no allegations suggesting that Brown (or anyone at SolarWinds) perceived any ongoing threat after the Company “changed the password” and “fixed the issue within the same hour it was reported,” more than a year before the Cyberattack was reported. Compl. ¶ 112; *see also Heartland*, 2009 WL 4798148, at *8.

C. Thornton-Trump’s presentation does not support an inference of scienter.

The SolarWinds Defendants have shown that, even assuming that Defendant Thompson learned about Thornton-Trump’s April 2017 presentation, nothing pled about the presentation conflicts with the statements Plaintiff claims misled investors, and thus those allegations cannot support a strong inference that Thompson acted with severe recklessness, much less an intent to

⁸ Where a plaintiff selectively quotes a document, it is entirely appropriate for the Court to consider the entire document in assessing plaintiff’s allegations. *See In re New Century*, 588 F. Supp. 2d 1206, 1221 (C.D. Cal. 2008).

deceive. *See* Def. Br. at 19–20. In response, Plaintiff argues that the presentation raises a strong inference of scienter because it asserts that SolarWinds’ “infrastructure and corporate systems exist in a precarious state” and that the Company lacked “centralized” security reporting and management and had “silos of communication.” *Opp.* at 53 & 57. These arguments fail for multiple reasons.

Simple examination of the complete relevant context surrounding the “precarious state” comment makes clear that it was not an indictment of SolarWinds’ security measures (either generally or, more to the point, with respect to any topic addressed by the specific statements Plaintiff challenges), but rather an acknowledgment of the ever-present threat of cyberattack that *all companies* face and about which SolarWinds repeatedly warned investors (*see* Def. Br. at 7–8 & n.8; *id.* at 19 & n.17 & n.18). The presentation said that “[o]ur security solutions, SaaS infrastructure and corporate systems exist in a precarious state – one moment we are secure and the next moment we are vulnerable.” Biles Decl. Ex. 24 at 13. Rather than alleging shortcomings in *SolarWinds*’ security measures or contradicting any challenged statement describing them, the presentation next cited the high-profile exploitation of a vulnerability in software *developed by another entity (Apache)* to compromise systems of over 500 users of the Apache software, as an illustration of the pervasive threat of cyberattack. *Id.* Where a plaintiff relies on isolated excerpts of a document, “the Court can view any statement selectively quoted or referenced in the context from which it was drawn to protect against any misrepresentation or misinterpretation.” *New Century*, 588 F. Supp. 2d at 1221. Read in its actual context, the “precarious state” comment merely echoes SolarWinds’ own public warnings about cybersecurity threats and risks. *See, e.g.*, Biles Decl. Ex. 7, 10/18/18 Prospectus at 25–26 (“Our systems and those of our third-party service providers are vulnerable to ... computer “hackers,” malicious code..., employee theft or misuse, and denial-of-service attacks, as well as sophisticated nation-state and nation-state-supported actors”). As such, it cannot support an inference that Thompson or any Defendant spoke with intent to deceive or severe recklessness.

The allegations of “No centralized reporting,” “No centralized management,” and “Silos of communication” fare no better. Plaintiff must plead facts that support a strong inference that the SolarWinds Defendants spoke with knowledge or severely reckless disregard that *their statements* would *mislead investors*.⁹ But Plaintiff does not argue that these allegations (i) conflict with any of the challenged statements (which addressed different topics) or (ii) raise a strong inference that the statements were made with severe recklessness. That failure alone is dispositive. Even if the Court were to infer that Thompson spoke with knowledge of internal allegations that SolarWinds lacked “centralized” security reporting and management and had “silos of communication” on security matters, that would not raise a strong inference that he acted with scienter.¹⁰

Plaintiff absurdly claims that this is all somehow “irrelevant” because the presentation purportedly placed the SolarWinds Defendants “on notice that SolarWinds was not secure.” Opp. at 57. That argument misapprehends the scienter analysis entirely. The challenged statements did not claim that SolarWinds’ systems were “secure.” To the contrary, the Company cautioned investors that its systems were “vulnerable” to the omnipresent risk of cyberattack and warned that “[t]he risk of a security breach or disruption, particularly through cyberattacks or cyber intrusion, including by computer hacks, foreign governments, and cyber terrorists, has generally increased in number, intensity and sophistication of attempted attacks, and intrusions around the world have increased.” See, e.g., Biles Decl. Ex. 7, 10/18/18 Prospectus at 25–26 (emphasis added); see also Ex. 13, 2/25/19 10-K at 15; Ex. 14, 2/24/20 10-K at 15. To the extent that the “centralized” management and “silos of communications” allegations somehow can be construed to suggest any Defendant’s awareness of

⁹ See *Tuchman v. DSC Commc’ns Corp.*, 14 F.3d 1061, 1069 (5th Cir. 1994); *Abrams*, 292 F.3d at 432–33.

¹⁰ See *In re Marriott*, 2021 WL 2407518, at **35, 37 (allegations that defendants knew of “cybersecurity deficiencies” and “red flags” did not support inference of scienter where the matters alleged did not conflict with challenged statements or suggest they were made with intent to deceive or severe recklessness).

risks that SolarWinds's systems were "not secure," the allegations would still fail to raise an inference of scienter.¹¹

Throughout the Opposition, Plaintiff strives to liken this case to *In re Equifax Inc. Sec. Litig.*, where the plaintiff pled facts demonstrating that the attacker accessed Equifax's internal systems by exploiting "poor authentication measures and inadequate network monitoring"—deficiencies that allegedly were exploited in earlier data incidents and cited in multiple security audits and investigations. *See* 357 F. Supp. 3d 1189, 1238 (N.D. Ga. 2019) ("The Amended Complaint details how these prior incidents were the result of many of the same problems that contributed to the Data Breach here.") Still, the *Equifax* court dismissed the claims against all but one of the individual defendants because plaintiff failed to allege that they "knew, or were severely reckless to the fact that, these prior breaches were symptomatic of fundamental security problems." *Id.* ("Without knowing that these [prior] breaches were specifically caused by authentication and network monitoring issues, these Defendants would not have been put on notice that there were shortcomings in these areas of security."). The allegations here are far weaker than the allegations found insufficient in *Equifax*. Plaintiff does not allege that the security deficiencies asserted here resulted in prior cyberattacks at SolarWinds. Nor does Plaintiff plead any facts specifying how the SVR perpetuated the Cyberattack on SolarWinds or linking the alleged cybersecurity deficiencies to the Cyberattack (indeed, documents on which Plaintiff relies confirm the absence of any link, *see supra* at 7). Thus, even if Plaintiff had sufficiently pled the Individual Defendants' awareness of the alleged cybersecurity deficiencies (it has not), Plaintiff has not pled that the Individual Defendants knew or recklessly disregarded that those alleged deficiencies

¹¹ *See In re Marriott*, 2021 WL 2407518, at *37 (holding that, plaintiff's allegations "support an inference that Defendants should have been aware of the risk of a cyber-attack . . . , but . . . do not support an inference that any of Defendants' statements were made with knowledge or with reckless disregard that they were false or misleading," particularly where "Marriott repeatedly disclosed that it was at risk of a cyber-attack").

were symptomatic of fundamental security problems making the challenged statements misleading. The Complaint thus fails to raise a strong inference of scienter. *See Equifax*, 357 F. Supp. 3d at 1238.

D. Hindsight allegations that SolarWinds delayed spending on cybersecurity fail to plead scienter.

Extrapolating backwards from post-Class Period estimates of costs for cybersecurity enhancements SolarWinds implemented following the Cyberattack, Plaintiff argues that incurring those expenses earlier would have caused SolarWinds to miss Wall Street analysts' earnings estimates for earlier periods and that this somehow supports an inference of scienter. *Opp.* at 58. The SolarWinds Defendants' opening brief showed why these speculative and hindsight-driven allegations fail to raise any inference of scienter—there are no allegations suggesting either (i) the need for, or (ii) the anticipated costs of the enhancements announced post-Cyberattack were known when the challenged statements were made, much less that the SolarWinds Defendants also knew that incurring those costs in earlier periods would mean missing earnings estimates. *See Def. Br.* at 29.

The Opposition fails to address these fatal deficiencies and instead cites inapposite cases involving allegations that are entirely different from those here. *Opp.* at 58. In *In re Akorn, Inc. Sec. Litig.*, plaintiffs alleged that defendants knew of financial controls deficiencies because, among other reasons, their auditors identified them, but they fired the auditors and refused to address the problems, eventually resulting in a restatement that reduced net income for an affected year by 194.7%. 240 F. Supp. 3d 802, 819–20 (N.D. Ill. 2017). In *In re AFC Enters., Inc. Sec. Litig.*, plaintiffs adequately pled a CFO's scienter by alleging his personal involvement in accounting manipulations to meet analysts' earnings expectations. 348 F. Supp. 2d 1363, 1375 (N.D. Ga. 2004).¹² Neither of these cases is remotely similar to this case; nor do they support for an inference of scienter here.

¹² Notably, the *AFC* court held that plaintiff failed to plead scienter as to several individuals because plaintiff did not allege they were aware that the company had purportedly cooked its books to meet earnings estimates. *Id.* at 1374.

Finally, Plaintiff's allegations about the security initiatives that SolarWinds implemented after the Cyberattack fail to support a strong inference that the Individual Defendants acted with scienter. These alleged reforms do not show that SolarWinds previously lacked "basic cybersecurity," nor do they show belated adoption of controls that SolarWinds claimed already to have in place. For example, Plaintiff argues that SolarWinds' creation of a Chief Information Security Officer ("CISO") position shows that only after the Class Period did SolarWinds "finally" "invest[] in developing a security team." Compl. ¶ 171. But the "new" CISO is none other than Tim Brown (*see* Biles Decl. Ex. 32, iTWire (March 29, 2021)), who Plaintiff acknowledges served as SolarWinds' VP of Security since 2017—over one year before the Class Period began. An upgrade to Brown's job title is not a basis for inferring scienter on the part of any Defendant. Nor do the other alleged post-Class Period measures, including the creation of a Board-level Technology and Cybersecurity Committee (Compl. ¶ 172), multi-factor authentication requirements (*id.* ¶ 173), redoubled efforts to ensure compliance with password and "least privilege" policies (*id.* ¶¶ 173–74), and unspecified enhancements to "lock[] down access to our environments" (*id.* ¶ 175), conflict with any of the challenged Class Period statements. This distinguishes SolarWinds' post-Cyberattack security enhancements from the *misleading accounting practices* discovered by the incoming CEO in *New Century*. *See* 588 F. Supp. 2d at 1231.¹³ The allegations about post-Cyberattack measures fail to support a strong inference of scienter.

II. PLAINTIFF PLEADS NO MATERIAL FALSE OR MISLEADING STATEMENT.

A. Plaintiff fails to plead that the Security Statement was false or misleading.

Plaintiff contends that SolarWinds' Security Statement was false or misleading because SolarWinds lacked certain cybersecurity protections described in the Statement. *See* Opp. at 26–27.

¹³ And Plaintiff's allegations are a far cry from those in *In re Resideo Techs., Inc., Sec. Litig.*, where "multiple confidential witnesses ... attest[ed] to the Defendants' knowledge of the relevant information that the Defendants failed to disclose." Case No. 19-cv-2863 (WMW/KMM), 2021 WL 1195740, at *6 (D. Minn. Mar. 30, 2021).

But the Complaint lacks the factual allegations to support this claim. To start, Plaintiff has not overcome the internal contradictions in its own allegations regarding the Security Statement:

- Plaintiff has not reconciled its claim that SolarWinds “had no security team,” Opp. at 26, with its acknowledgment that Brown was “SolarWinds’ Vice President of Security Architecture since 2017.” Compl. ¶ 16. The point is not that Brown was a “team of one,” Opp. at 32, but rather that it is not plausible to infer (and Plaintiff has pled no facts to show) that he led a department with no members.
- The allegation that SolarWinds did not conduct employee background checks does not show that it did not follow the NIST Cybersecurity Framework. *See* Compl. ¶ 57. The Framework does not require background checks, *see supra* at 4 n.6, and plaintiff has not pled facts supporting an assertion that the statement about the NIST Framework was false or misleading.

Plaintiff’s other factual allegations—drawn from Thornton-Trump and the FEs—fare no better. For reasons explained in the SolarWinds Defendants’ opening brief at 34–36, these allegations fail to plead with the factual particularity the PSLRA requires that the challenged statements falsely or misleadingly described SolarWinds’ cybersecurity posture during the Class Period.

B. Plaintiff has not pled that optimistic opinion statements about SolarWinds’ cybersecurity were material.

Plaintiff also argues that general statements about SolarWinds’ security—such as: Brown’s security team “focuses on” security hygiene, *id.* ¶¶ 220, 222, SolarWinds applies “appropriate” security measures to handle customer data, *id.* ¶ 216, and security and privacy are “top priorities,” *id.* ¶ 218—are actionable. The law is clear that they are not. *See* Def. Br. at 36–37. A district court recently held similar statements to be either puffery or too vague to constitute material statements of fact. *See In re First Am. Fin. Corp. Sec. Litig.*, No. 20-9781, 2021 WL 4807648, *8-10 (C.D. Cal. Sept. 22, 2021).¹⁴ Any argument that these statements were materially misleading is further undercut by SolarWinds’

¹⁴ Contrary to Plaintiff’s claim that *First American* involved only “vague statements” that defendants were “committed” and “serious” about cybersecurity, Opp. at 31, the non-actionable statements in that case included representations that the issuer “restricts access to nonpublic personal information” and maintained “physical, electronic, and procedural safeguards that comply with federal regulations to guard [customers’] nonpublic personal information.” 2021 WL 4807648, at **15, 18.

repeated warnings about precisely the risk that materialized: a sophisticated cyberattack by nation-backed wrongdoers. *See* Def. Br. at 32; Biles Decl. Ex. 13, 2/25/19 10-K at 15. Plaintiff tries to wave away SolarWinds’ warnings as “boilerplate,” Opp. at 28, but Plaintiff’s cases involved inapposite facts and far more generic risk disclosures than SolarWinds made.¹⁵

III. PLAINTIFF FAILS TO PLEAD A CAUSAL LINK BETWEEN THE “CORRECTIVE DISCLOSURES” AND THE CYBERATTACK.

Plaintiff fails to plead loss causation because the alleged “corrective disclosures” on December 13-17, 2020 did not reveal any “truth” alleged to have been concealed or obscured by the challenged statements. Def. Br. at 38-40. As Plaintiff’s own authority establishes, the revelation of the Cyberattack itself does not correct the alleged misstatements concerning SolarWinds’ cybersecurity. *See Equifax*, 357 F. Supp. 3d at 1250 (“the plaintiff has failed to explain how the ‘materialization’ of the data breach itself corrected prior misstatements touting the strength of Equifax’s cybersecurity”). Thus, the disclosures on December 13 and 14, 2020—which simply announced the Cyberattack (Compl. ¶¶ 225-26) and did not discuss any alleged cybersecurity deficiencies at SolarWinds—did not correct any alleged misstatements.

While subsequent articles in the *Wall Street Journal*, *Reuters*, and *Bloomberg* criticized SolarWinds’ cybersecurity controls, including the “solarwinds123” password issue (Compl. ¶¶ 229-232), Plaintiff failed to plead a plausible causal link between any of these alleged deficiencies and the Cyberattack. *See* Def. Br. at 39–40. Plaintiff does not plead facts indicating that the SVR exploited any of the alleged cybersecurity deficiencies to perpetrate the Cyberattack on SolarWinds. The most Plaintiff offers is the insinuation that “until November 2019 [when SolarWinds discovered and disabled the “solarwinds123 password”], a malicious actor ***could have*** uploaded malware to the Update Server by

¹⁵ *See Lormand v. US Unwired, Inc.*, 565 F.3d 228, (5th Cir. 2009) (disclaimer “boilerplate” and not meaningful cautionary language under PSLRA safe harbor); *Jaroslavicz v. Me&T Bank Corp.*, 962 F.3d 701, 713–14 (3d Cir. 2020) (disclosures “offered information generally applicable to nearly any entity operating in a regulated environment”).

using the password “solarwinds123.” Opp. at 2 (emphasis added). This speculative allegation is not a well-plead fact that provides the requisite link between the alleged misstatements and the Cyberattack. *Pub. Emps. Ret. Sys. of Miss. v. Amedisys, Inc.*, 769 F.3d 313, 320 (5th Cir. 2014) (“the plaintiff must allege that when the ‘relevant truth’ about the fraud began to leak out ... it caused the price of the stock to depreciate.”). Moreover, documents that Plaintiff cites in the Complaint establish that the “solarwinds123” password issue ***had nothing to do with the Cyberattack***. See, e.g., *supra* at 7. Plaintiff fails to explain how the alleged security deficiencies at SolarWinds “relate to” the Cyberattack. *Amedisys, Inc.*, 769 F.3d at 321. Without facts showing a direct link between the deficiencies and the Cyberattack, Plaintiff’s allegations at most “touch upon” the Cyberattack, which is insufficient to plead loss causation. *In re Dell Inc., Sec. Litig.*, 591 F. Supp. 2d 877, 907–09 (W.D. Tex. 2008)(concluding that disclosures that merely “touch upon” the alleged fraud failed to meet the loss causation standard articulated by the Supreme Court in *Dura*).¹⁶

For these reasons, the Complaint fails to adequately plead the element of loss causation.

CONCLUSION

For the above reasons, and as set forth in the SolarWinds Defendants’ opening brief, the Complaint fails to satisfy the PSLRA’s pleading standards and should be dismissed with prejudice.

¹⁶ Plaintiff’s allegations stand in sharp contrast to those in the cases cited in the Opposition. For example, in *Equifax*, the alleged corrective disclosure revealed the cybersecurity vulnerability (failure to implement software patches) that allowed the hackers to conduct the data breach at issue, which was also (i) the cause of prior data breaches, and (ii) identified as a cybersecurity problem in multiple earlier audits and investigations. 357 F. Supp. 3d at 1250. Similarly, in *Amedisys*, the corrective disclosures included articles that questioned Amedisys’s accounting and billing practices and announcements of multiple government investigations into those same billing and accounting practices. 769 F.3d at 322–324. Amedisys later blamed disappointing financial results on a change to its billing practices in response to the investigation. *Id.* at 324 (“Once Amedisys was placed under the spotlight of government scrutiny for Medicare fraud, its earnings dropped significantly because its employees could no longer continue exploiting Medicare reimbursements.”). Thus, plaintiffs in *Amedisys* pled a direct link between the corrective disclosures and the challenged billing practices. The absence of such a link here requires dismissal of the Complaint.

Dated: November 1, 2021

Respectfully submitted,

/s/ Michael J. Biles

Paul R. Bessette

Texas Bar No. 02263050

Michael J. Biles

Texas Bar No. 24008578

KING & SPALDING LLP

500 W. 2nd Street, Suite 1800

Austin, TX 78701

Tel: (512) 457-2050

Fax: (512) 457-2100

pbessette@kslaw.com

mbiles@kslaw.com

*Counsel for SolarWinds Corp.,
and Tim Brown*

CERTIFICATE OF SERVICE

I certify that on November 1, 2021, all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF Filing System on all parties in this case.

/s/ Michael J. Biles

Michael J. Biles